XDef 2019

对话 · 交流 · 合作　　前沿 · 实用 · 人才

第八届全国网络与信息安全防护峰会

零信任—大数据时代的网络安全新架构

左英男
奇安信集团

1、新IT技术架构的安全挑战

2、零信任架构的发展历史

3、什么是零信任架构?

4、零信任架构的应用实践

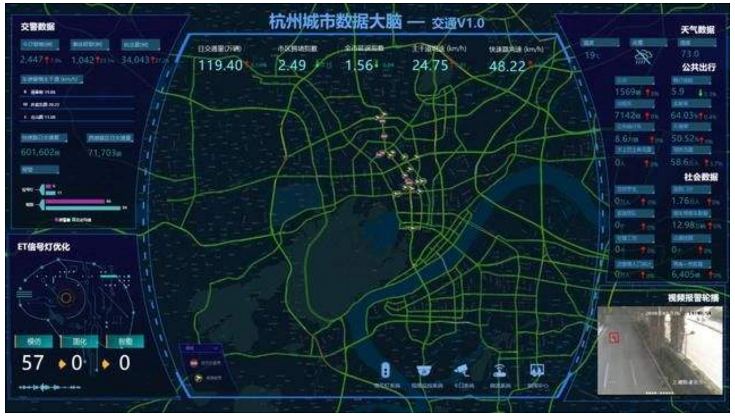
1、新IT技术架构的安全挑战

2、零信任架构的发展历史

3、什么是零信任架构?

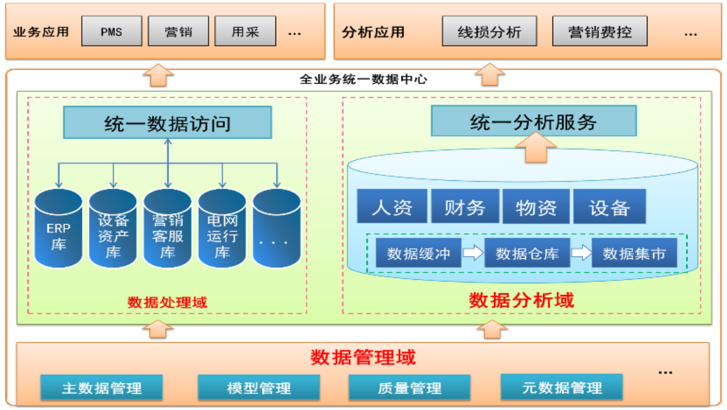
4、零信任架构的应用实践

以大数据为核心的新一代信息化建设浪潮



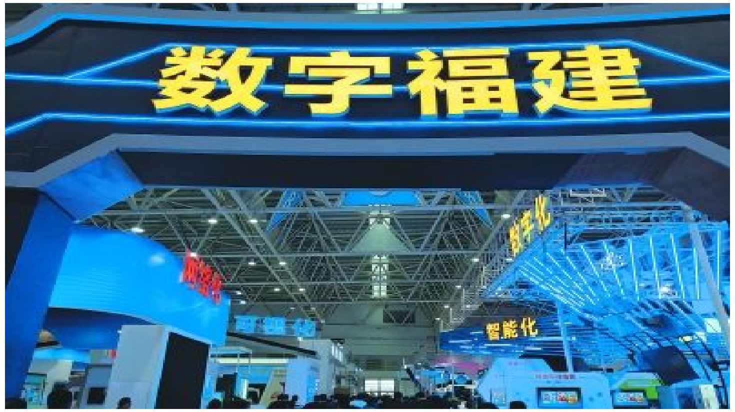
浙江杭州城市数据大脑

贵阳警方“人像大数据”系统



国家电网全业务统一数据中心

异地就医“全国一卡通”



政务数据整合汇聚与共享应用

综合交通出行大数据开放云平台

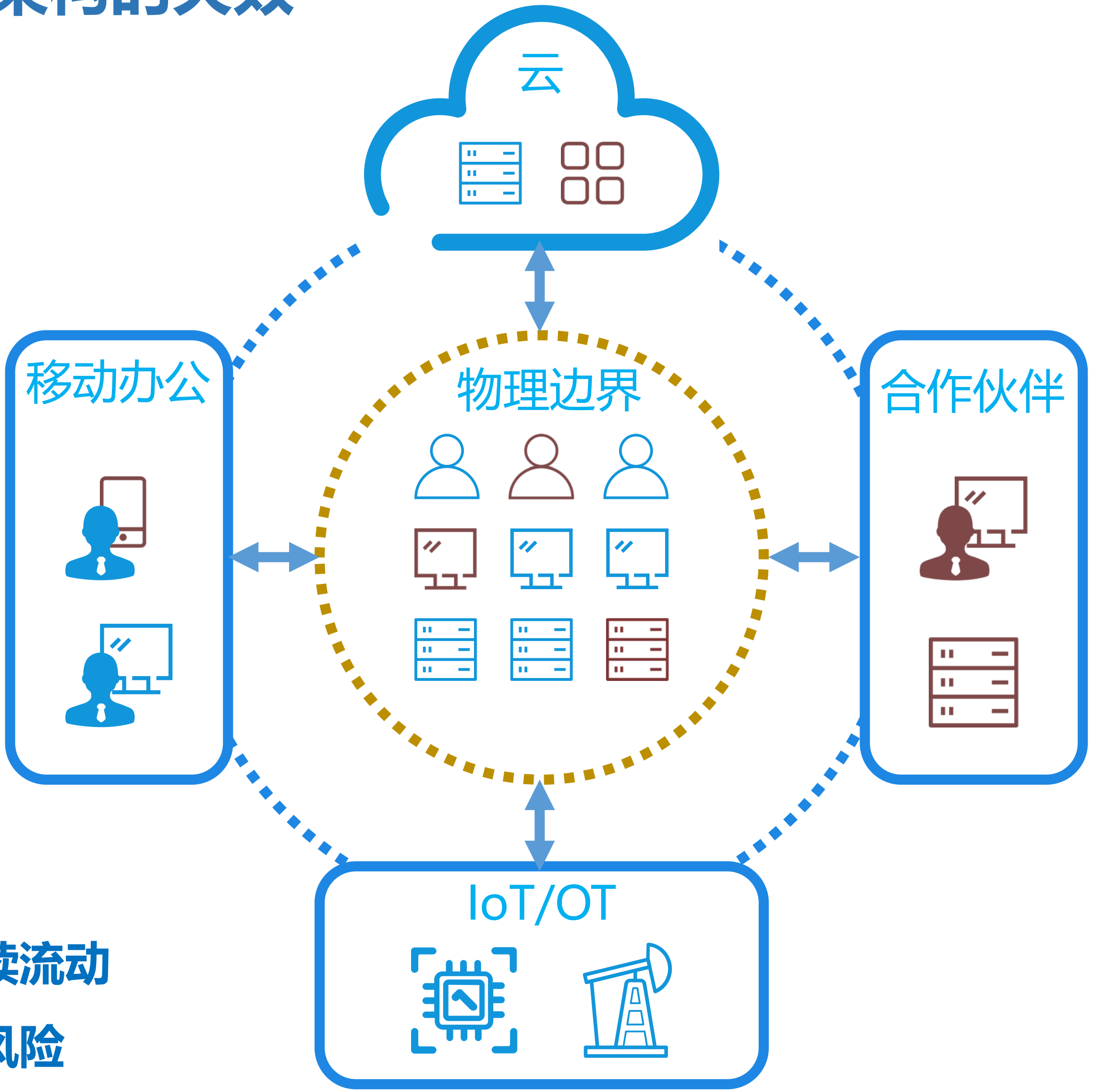
挑战1：新一代IT技术架构加剧了边界安全架构的失效

用户多样化

设备多样化

平台多样化

业务多样化

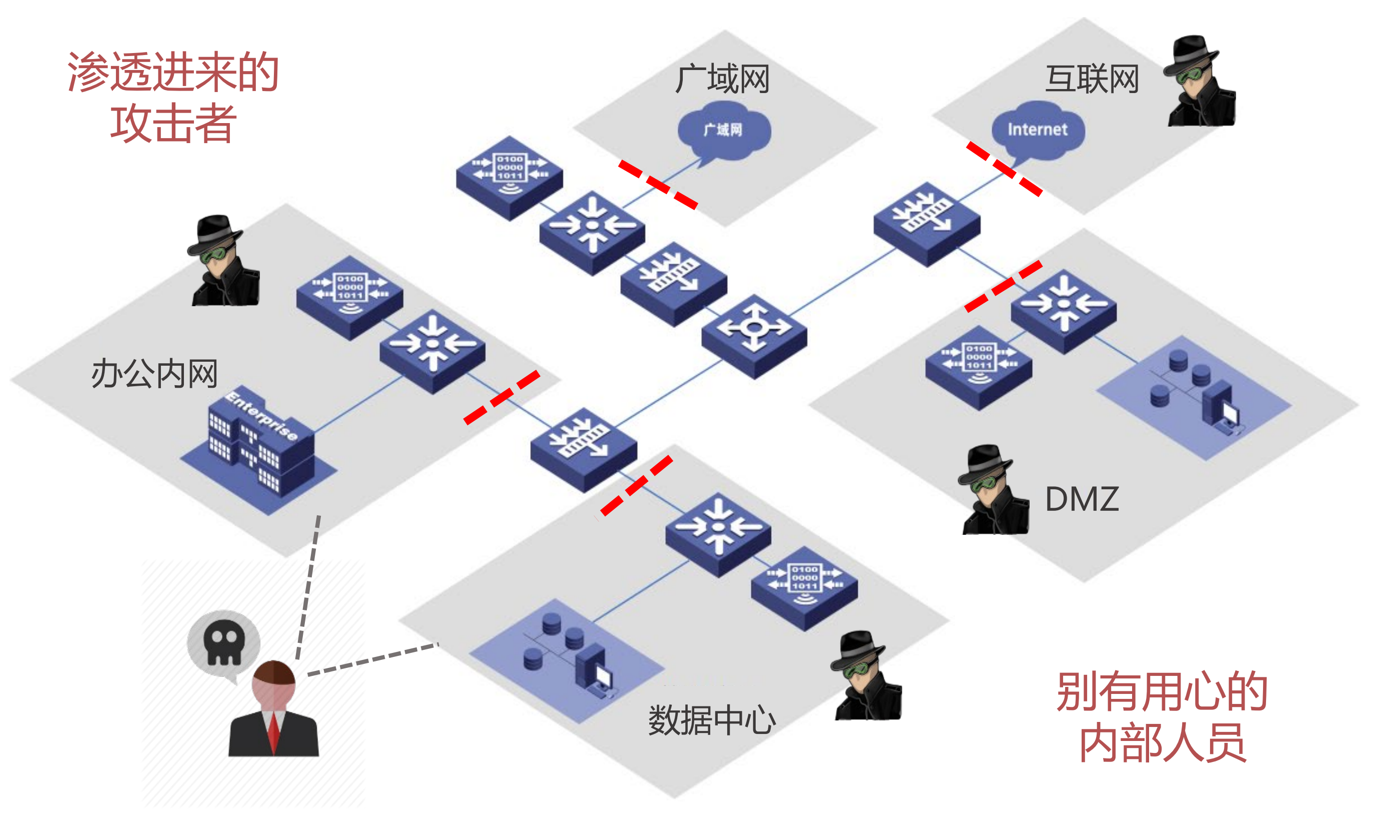


数据分散在不同的业务应用中并持续流动

数据的流动加剧了大数据的安全风险

挑战2：传统的边界安全架构忽视了内部威胁

安全意识？　　安全投入？　　安全措施？



边界安全架构：为内网中的人和设备预设了过多的信任

数据泄露“黑天鹅”事件背后
都隐藏着“灰犀牛”式的危机

零信任架构
Zero Trust Architecture

1、新IT技术架构的安全挑战

2、零信任架构的发展历史

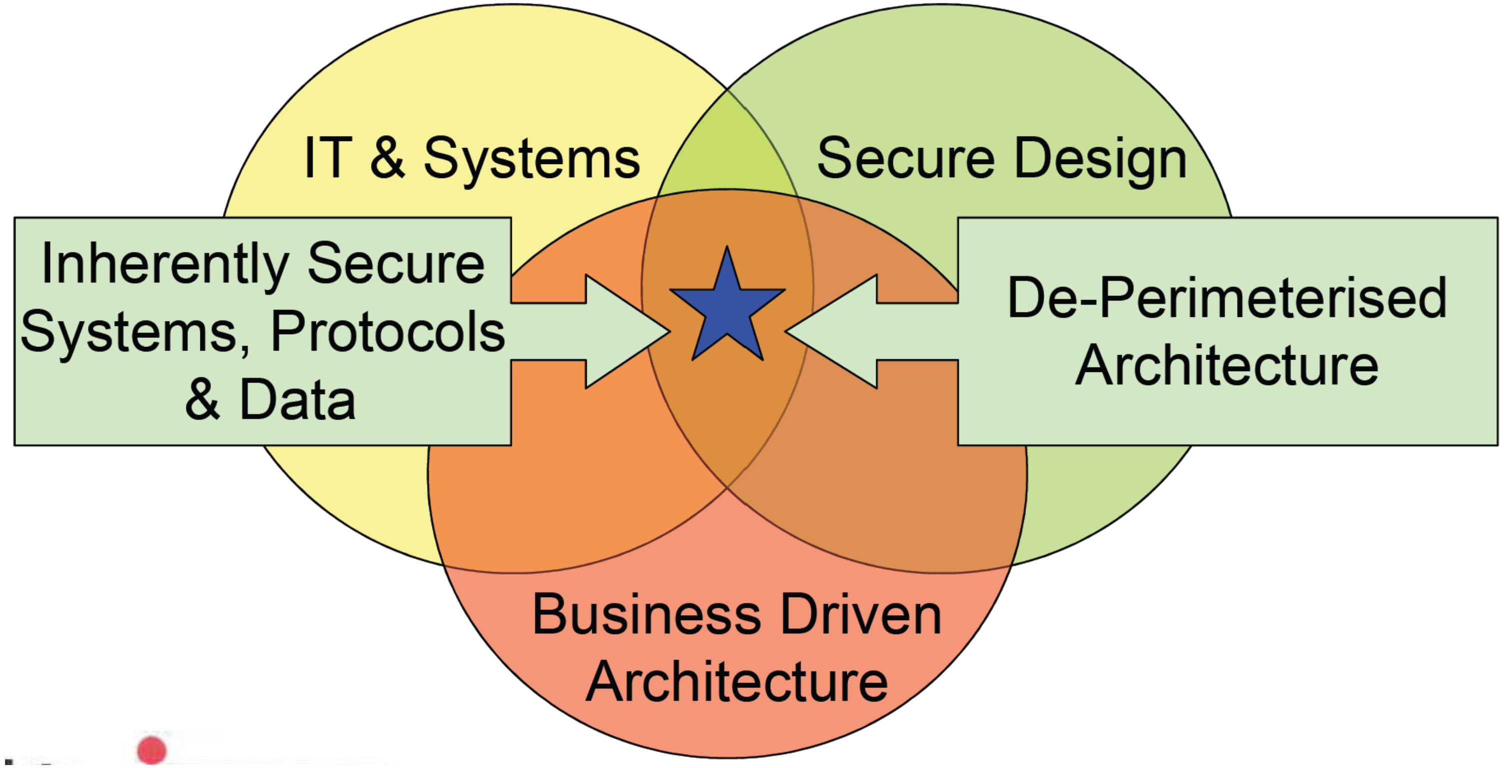
3、什么是零信任架构?

4、零信任架构的应用实践

发展简史：2005，Jericho Forum

JERICHO FORUM

BlackHat USA • EUROPE • ASIA USA 2005



* *"Inherent Security" - That everything is;*

- *Authenticated*
- *Protected against unauthorised reading (probably Encrypted)*
- *Repudiatable*

发展简史：2009，Forrester Zero Trust

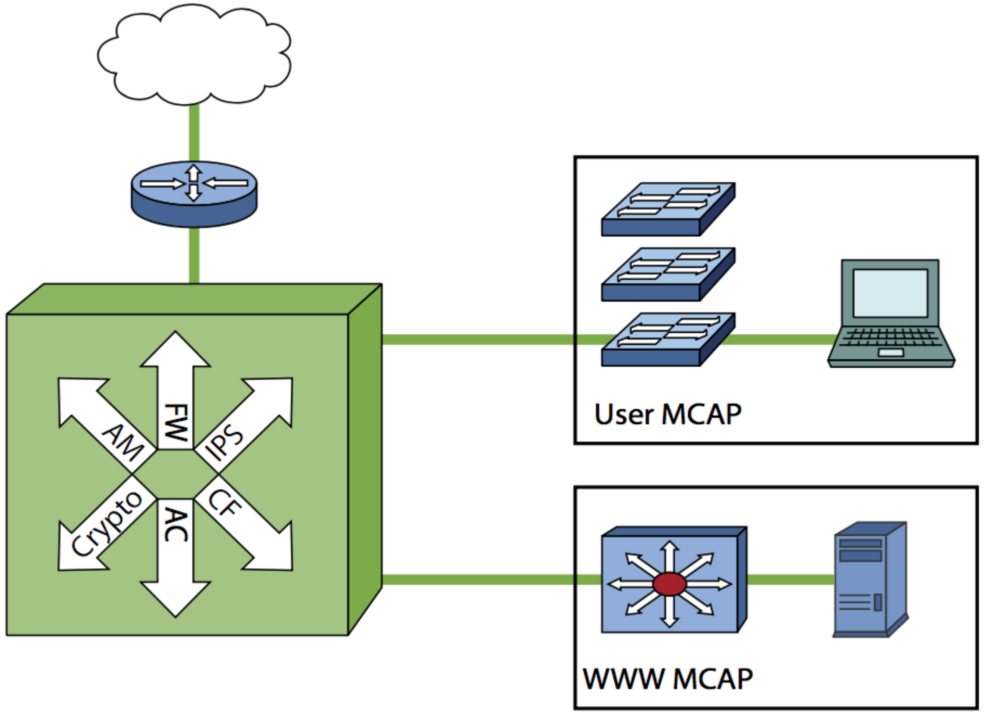
核心概念：

1、资源的安全访问和位置无关。

2、遵循最小权限原则并强制实施访问控制。

3、检测和记录所有流量

FORRESTER®



November 5, 2010

Build Security Into Your Network's DNA: The Zero Trust Network Architecture

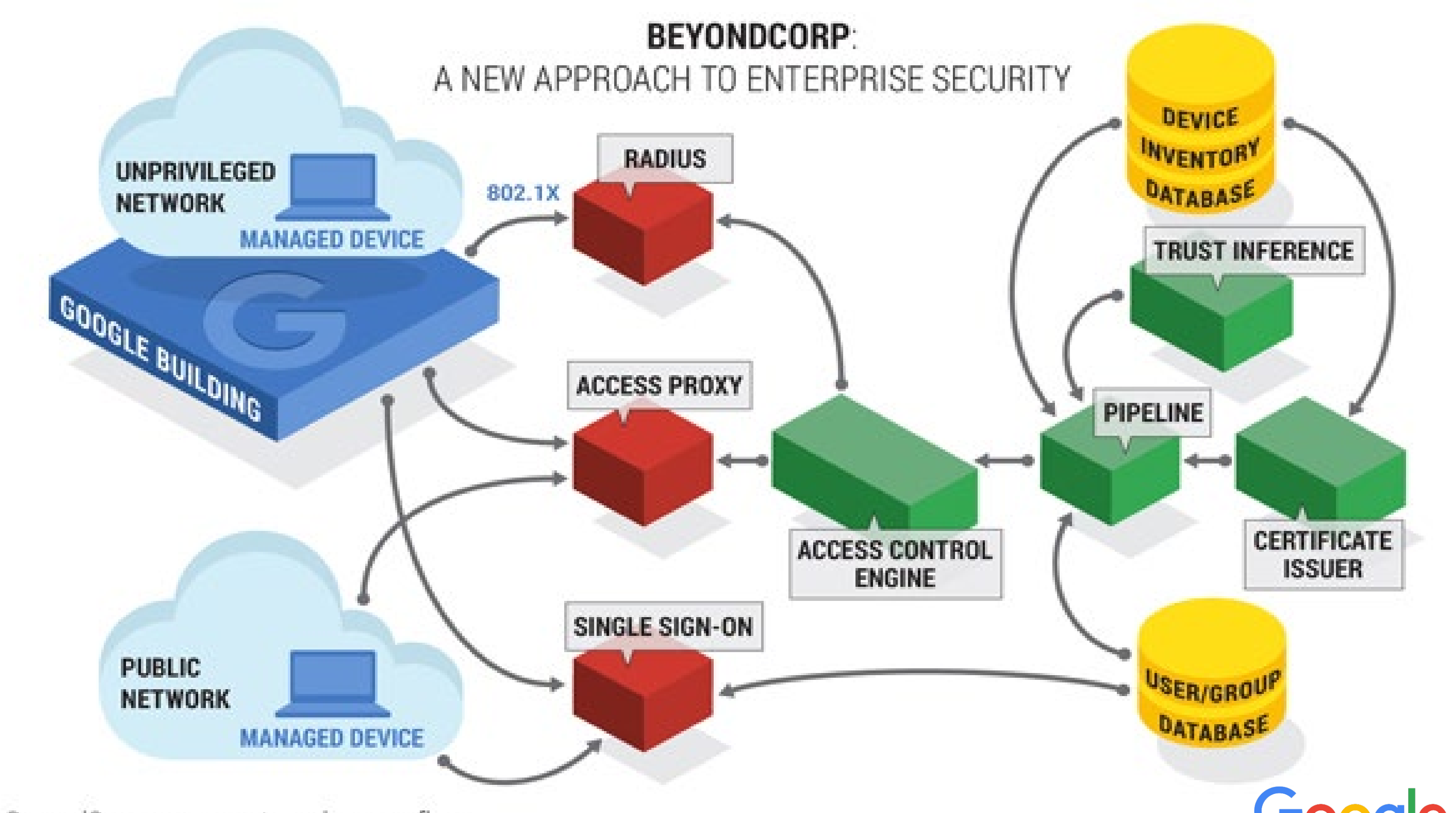
by John Kindervag

with Stephanie Balaouras and Lindsey Coit

发展简史：2017，Google BeyondCorp

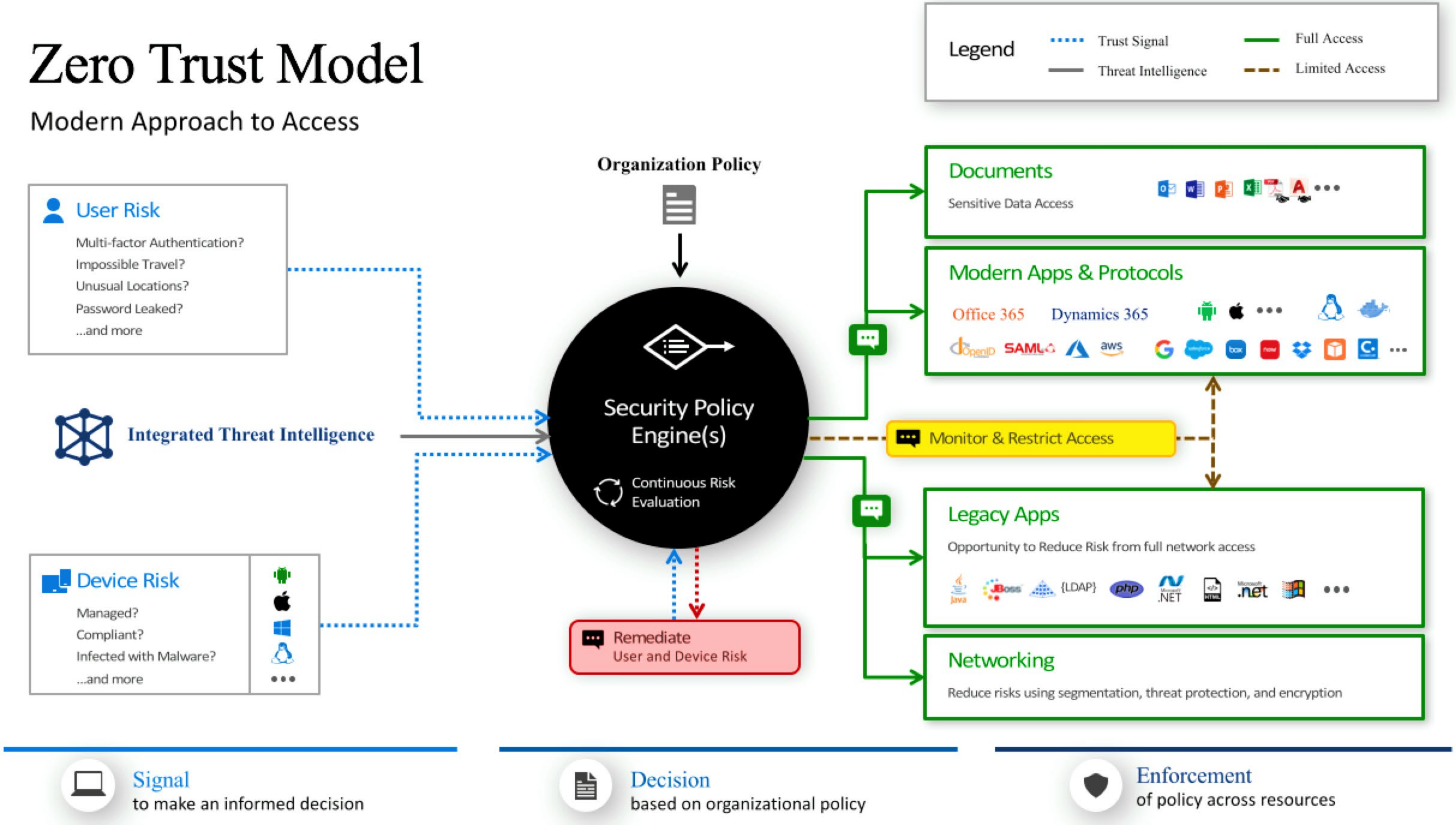
Google BeyondCorp是在构建零信任网络6年经验的基础上打造的新一代企业安全架构。

通过将访问权限控制措施从网络边界转移到具体的**设备、用户和应用**，让员工可以更安全地在任何地点工作，而不必借助于传统的VPN。

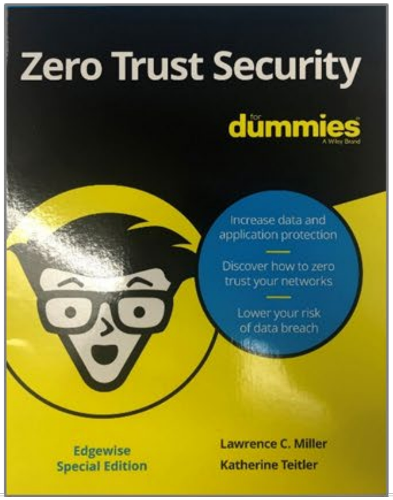


BeyondCorp components and access flow

发展简史：2018，Microsoft Zero Trust Model



2019年：3月，RSAC

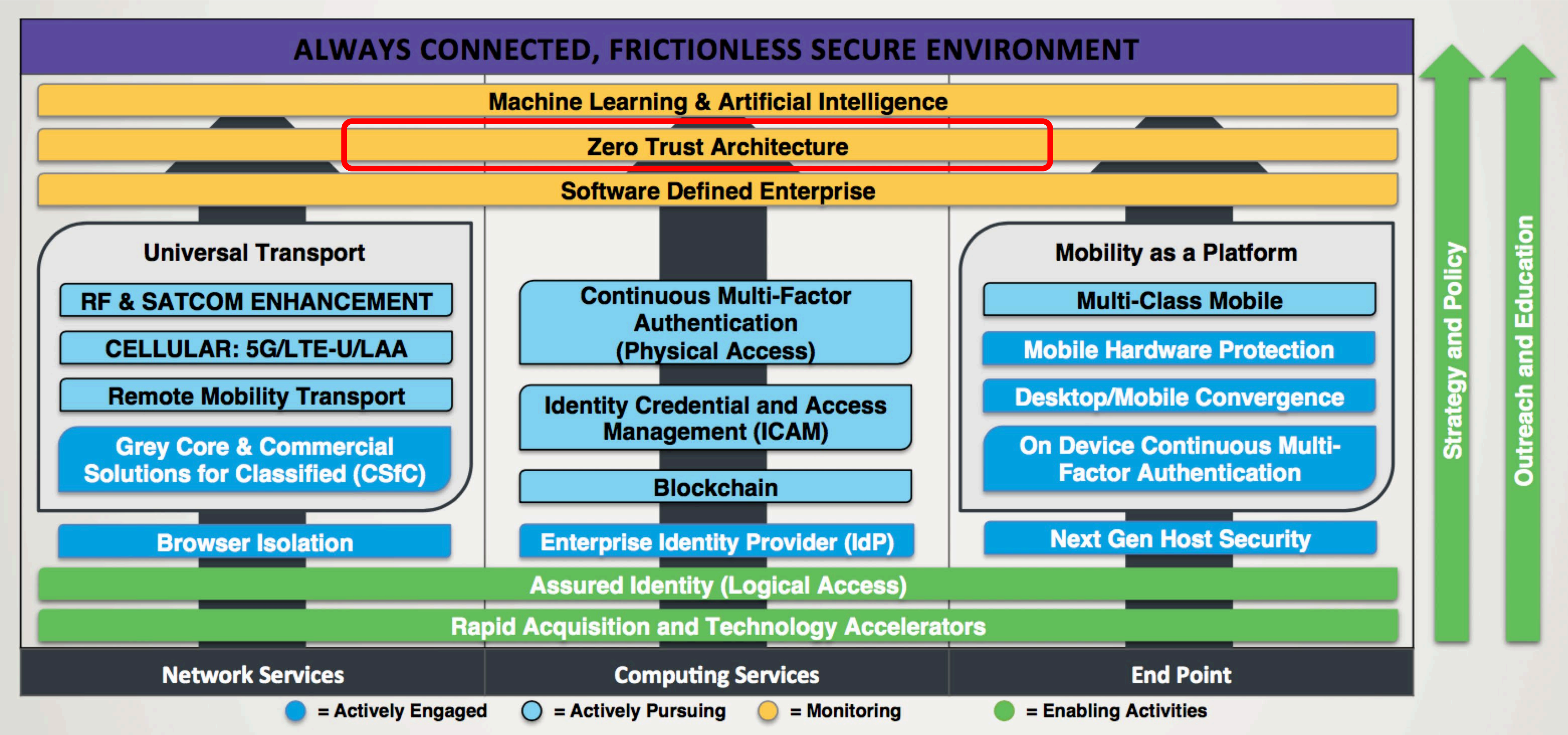


2019年：3月，RSAC

基础设施厂商	IAM厂商	传统安全厂商	创新安全公司	
Google	Centrify	Symantec	Luminate	Double Octopus
MS Azure	Okta	PAN	Aporeto	Guardicore
AWS	DUO	Zscaler	Cloud Harmonics	Jump Cloud
Akamai	Ping Identity	Tripwire	Cloudflare	Netronome
……	ForgeRock	AlgoSec	Cymbel	Plixer
	PulseSecure	MobileIron	Cyxtera	ScaleFT
	……	……	SecureCircle	idaptiv
			ArecaBay	Basil
			……	……

2019年：7月，美国国防信息系统局（DISA）战略规划2019-2022

DISA技术发展路线图



2019年：7月，《美国国防部数字现代化战略》

零信任安全的概念：

- 零信任是一种网络安全策略，它将安全嵌入到整个体系结构中，以阻止数据泄露。

零信任安全的优势：

- 这种以**数据为中心**的安全模型，消除了受信任或不受信任的网络、设备、角色或进程的概念，并转变为基于**多属性的信任级别**，使身份验证和授权策略在最小特权访问概念下得以实现。
- 实现零信任，需要重新思考我们如何利用现有的基础设施，以更简单、更高效的方式设计安全性，同时实现不受阻碍的操作。
- 除了总体上保护架构的优势外，还有其他跨功能的好处。

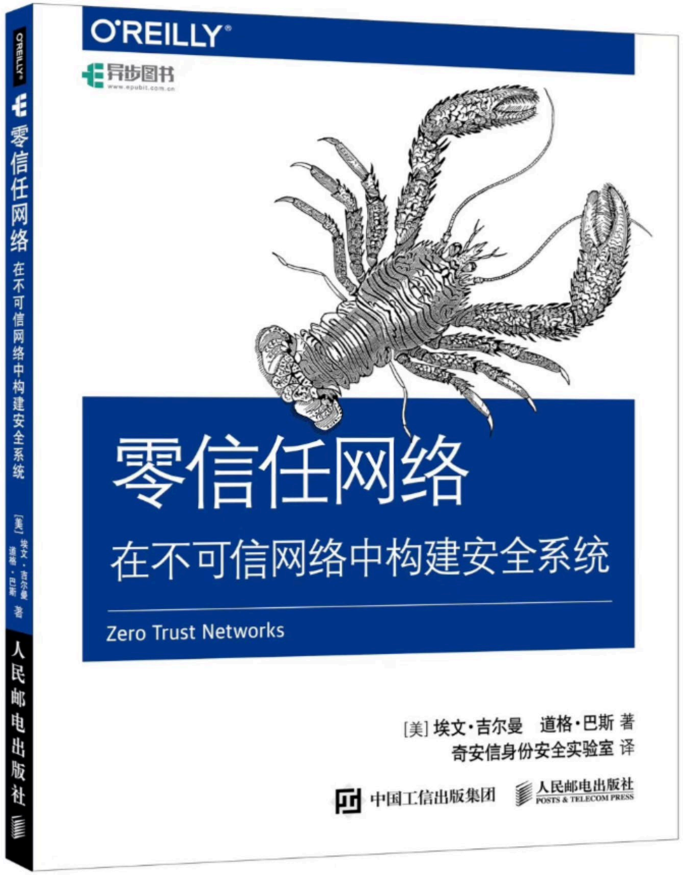
1、新IT技术架构的安全挑战

2、零信任架构的发展历史

3、什么是零信任架构?

4、零信任架构的应用实践

什么是零信任架构？在不可信的网络环境下重建信任



① 应该假设网络始终存在**外部威胁和内部威胁**，仅仅通过网络位置来评估信任是不够的。

② 默认情况下不应该信任网络**内部或外部**的任何人/设备/系统，而是基于**认证和授权**重构业务访问控制的信任基础。

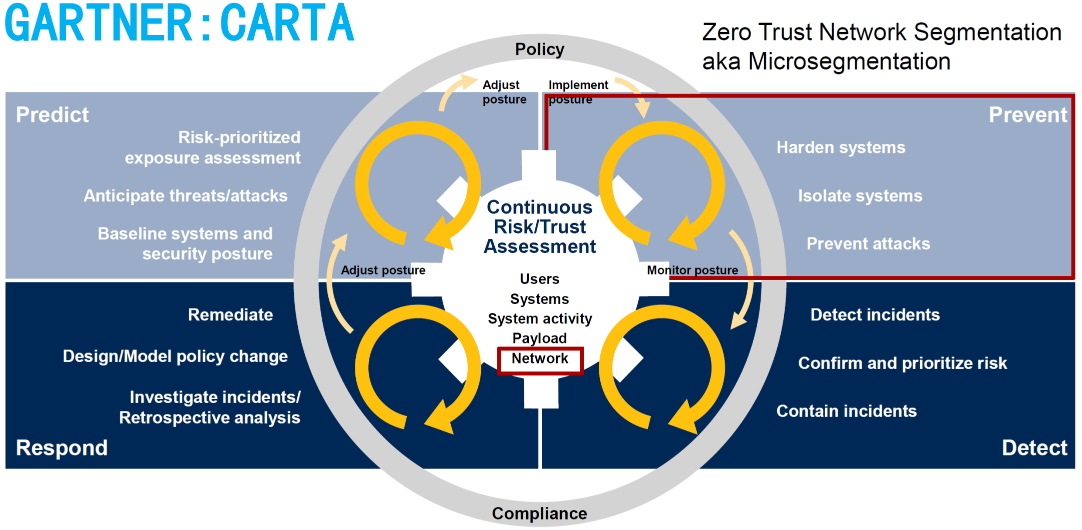
③ 每个设备、用户的业务访问都应该被**认证、授权和加密。**

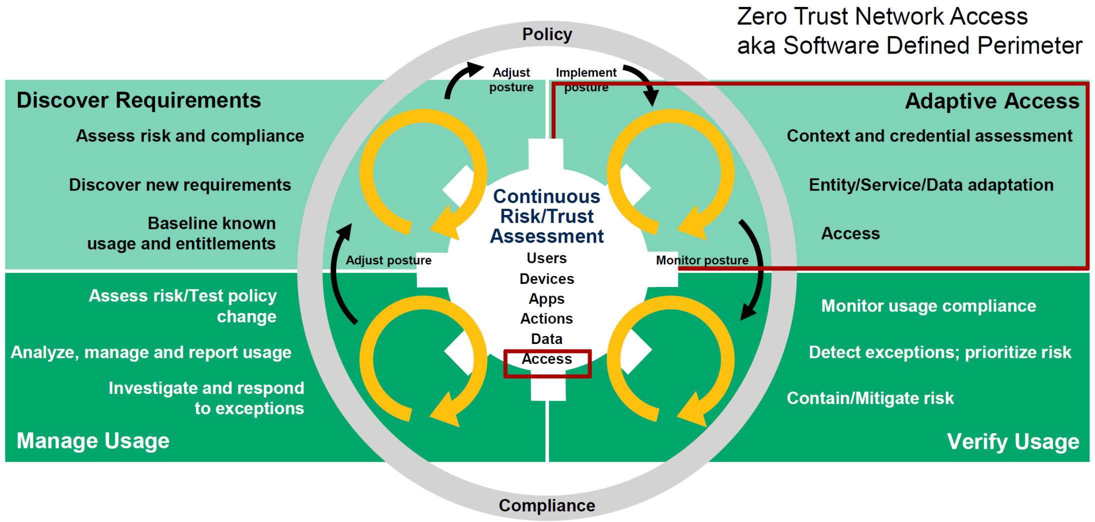
④ 访问控制策略和信任应该是**动态**的，基于设备、用户和环境的多源环境数据计算出来。

技术本质是构建以身份为基石的业务动态可信访问控制机制！

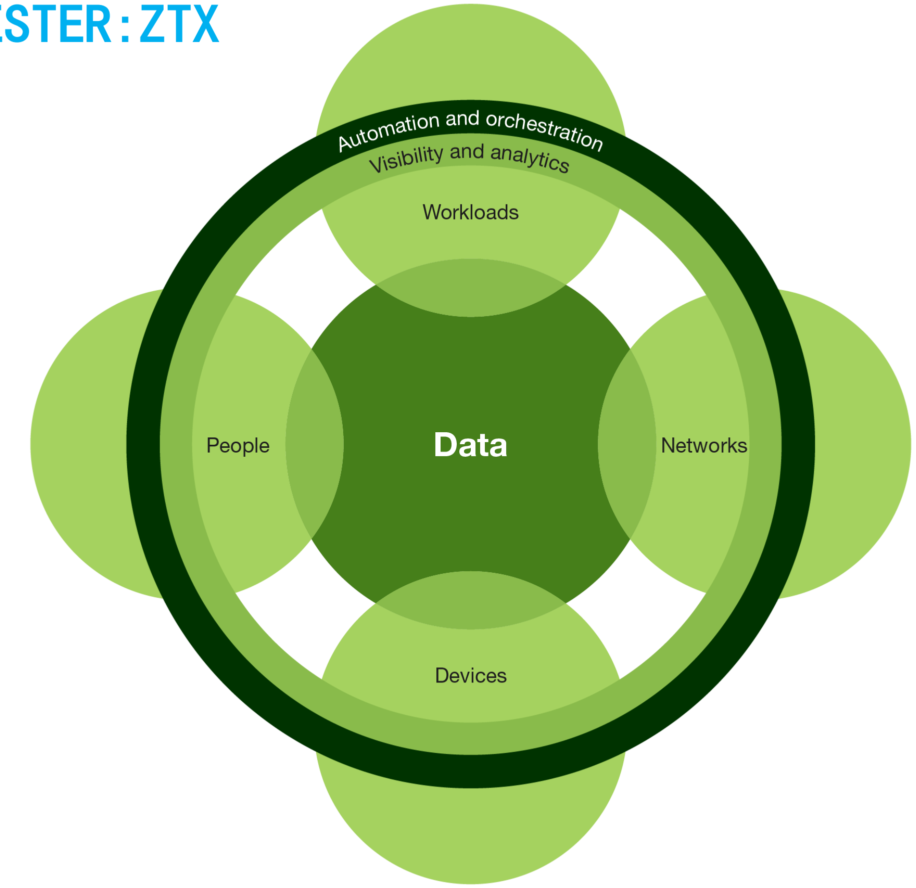
什么是零信任架构？Gartner vs. Forrester

GARTNER：CARTA





FORRESTER：ZTX



- **范围的扩展：** 网络 —> 用户、设备、工作负载
- **能力的扩展：** 微隔离—> 可视、分析、自动化、编排

什么是零信任架构？美国NIST《零信任架构》草案

Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207-draft

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

2019年9月

零信任架构是一种端到端的网络安全体系，包含身份、凭据、访问管理、操作、终端、托管环境与关联基础设施。零信任架构提供了相关概念、思路和组件关系的集合，旨在**消除在信息系统和服务中实施精准访问策略的不确定性**。

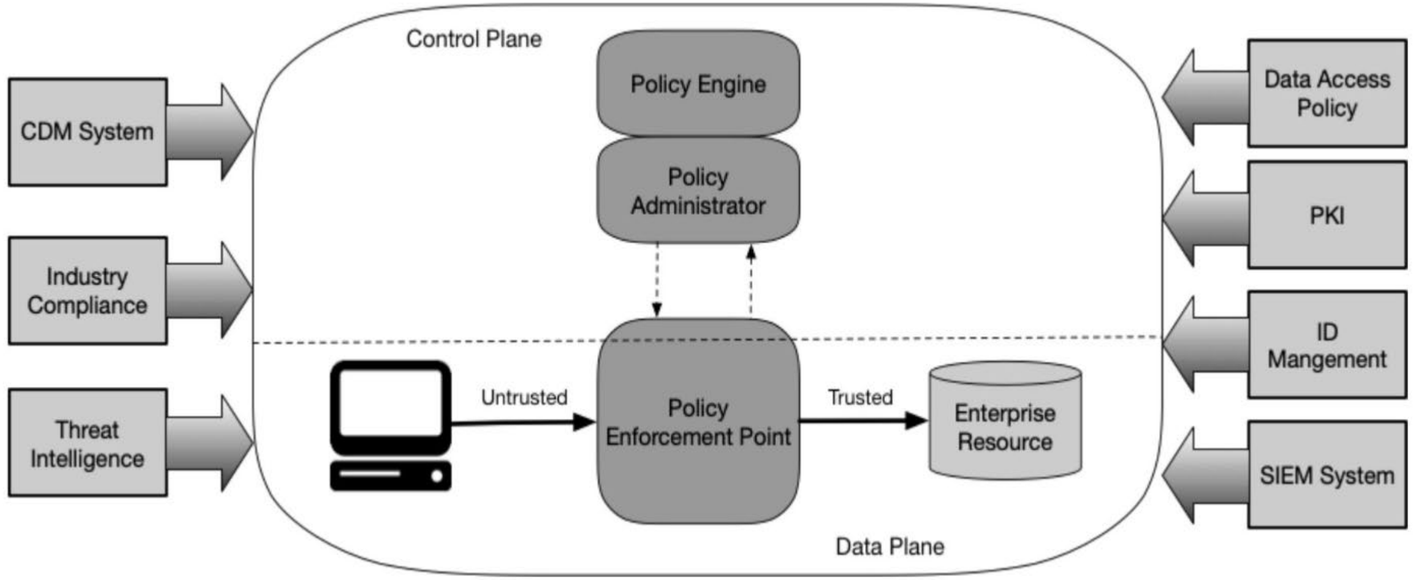
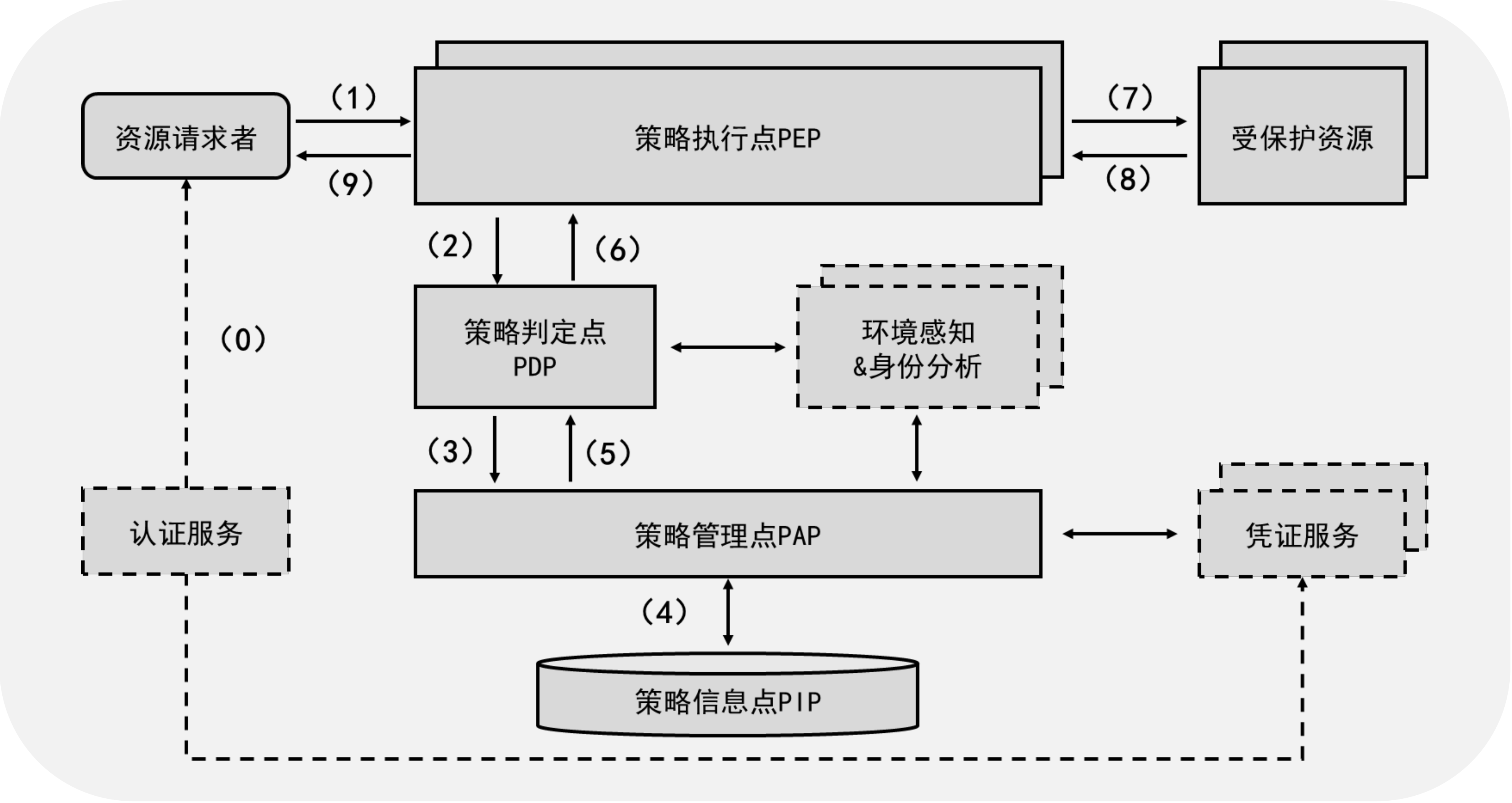


Figure 2: Core Zero Trust Logical Components

什么是零信任架构？Next Generation Access Control



什么是零信任架构？ Why now?

攻防 vs. **控制**

威胁驱动演进 架构驱动演进

★ 恶意代码 ★ 访问控制

Mainframe vs. Internet vs. Cloud

rwxrwxrwx 防火墙 零信任

最小权限

JIT(Just In Time) & JEA(Just Enough Access)

1、新IT技术架构的安全挑战

2、零信任架构的发展历史

3、什么是零信任架构?

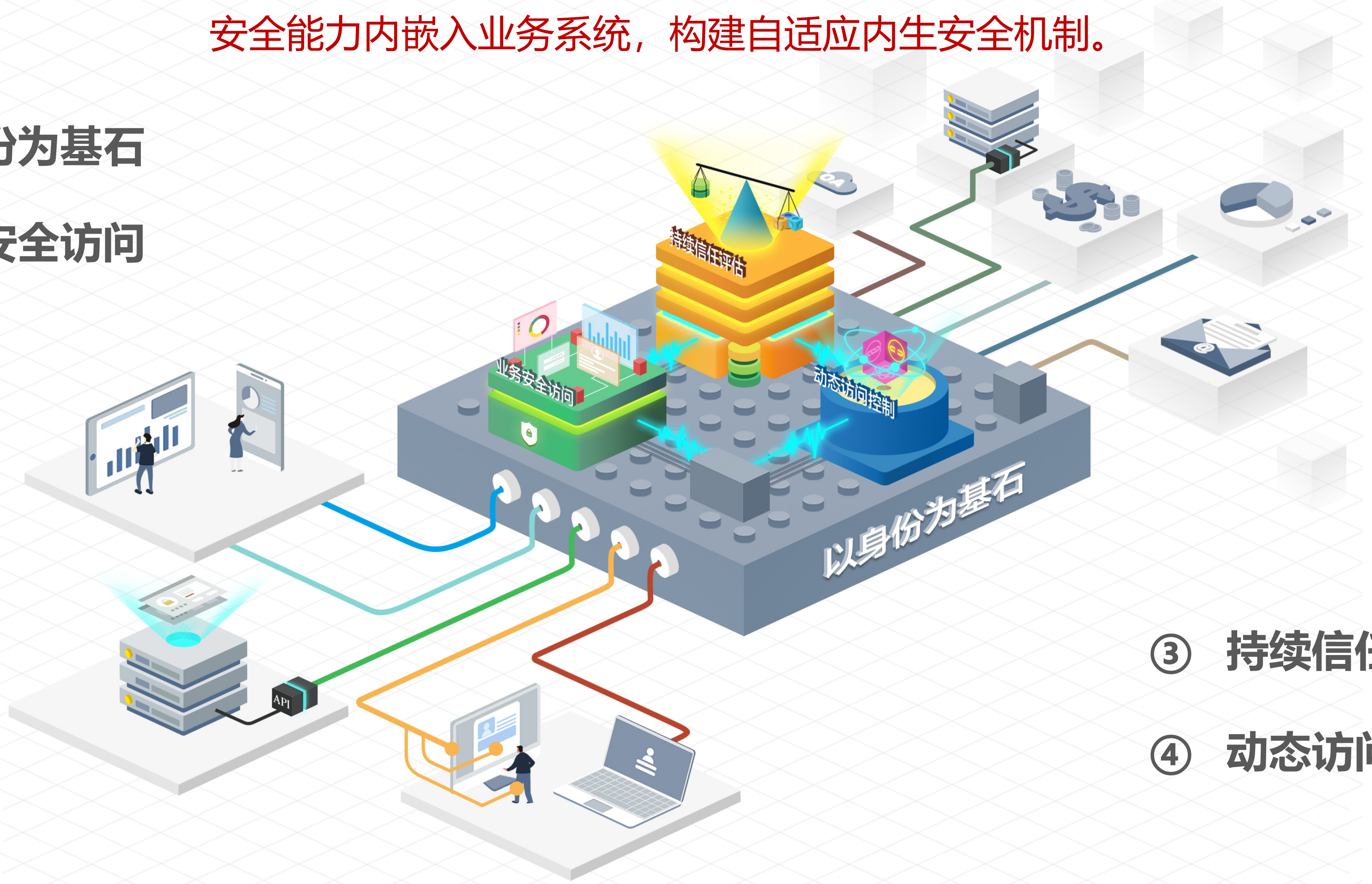
4、零信任架构的应用实践

奇安信对零信任的解读

安全能力内嵌入业务系统，构建自适应内生安全机制。

① 以身份为基石

② 业务安全访问



③ 持续信任评估

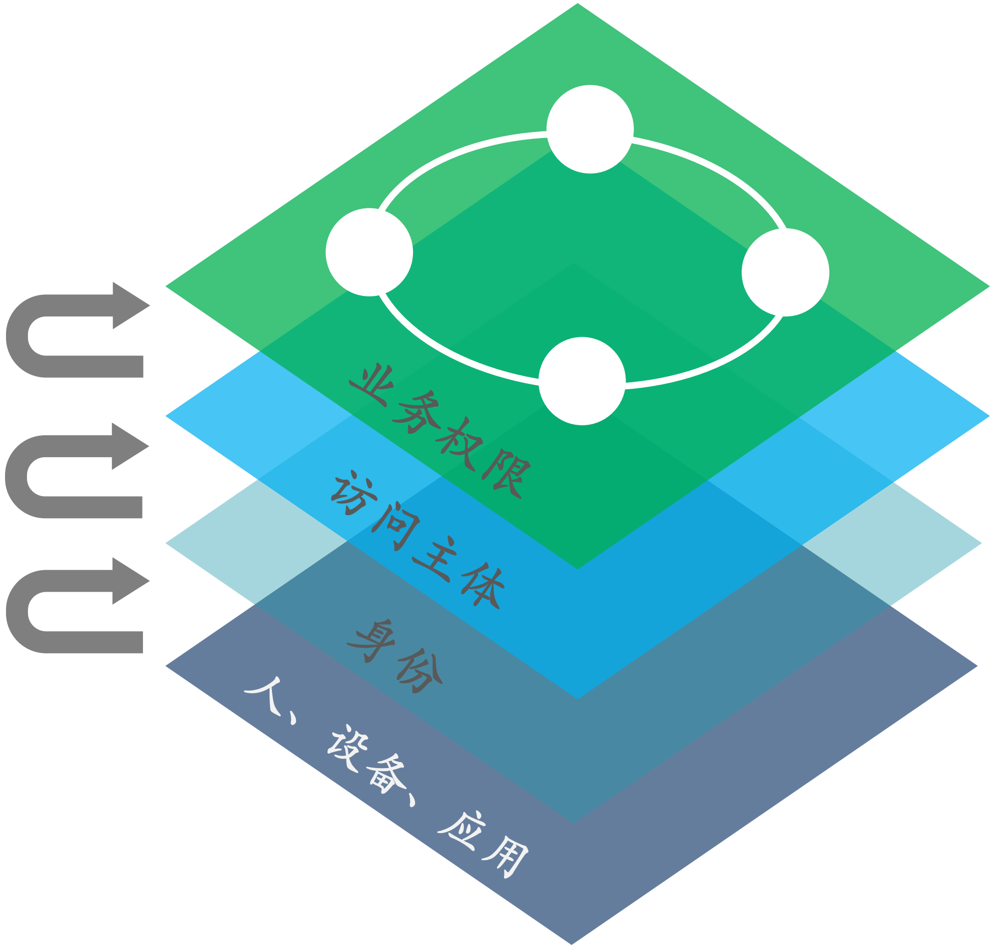
④ 动态访问控制

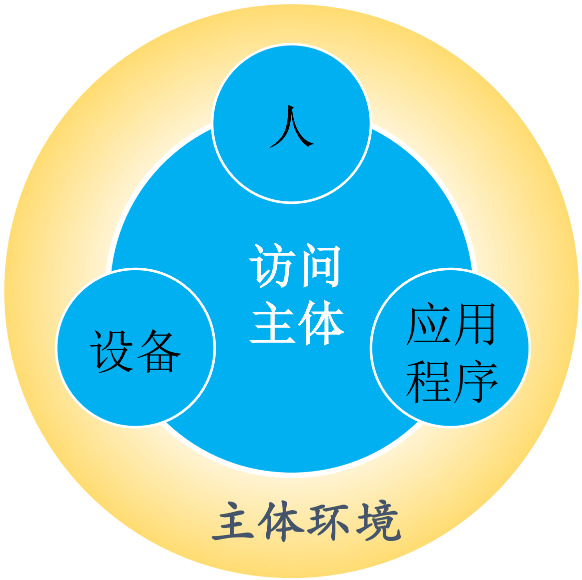
以身份为基石

为访问主体
设定最小权限

为数字身份
构建访问主体

为人和设备
赋予数字身份

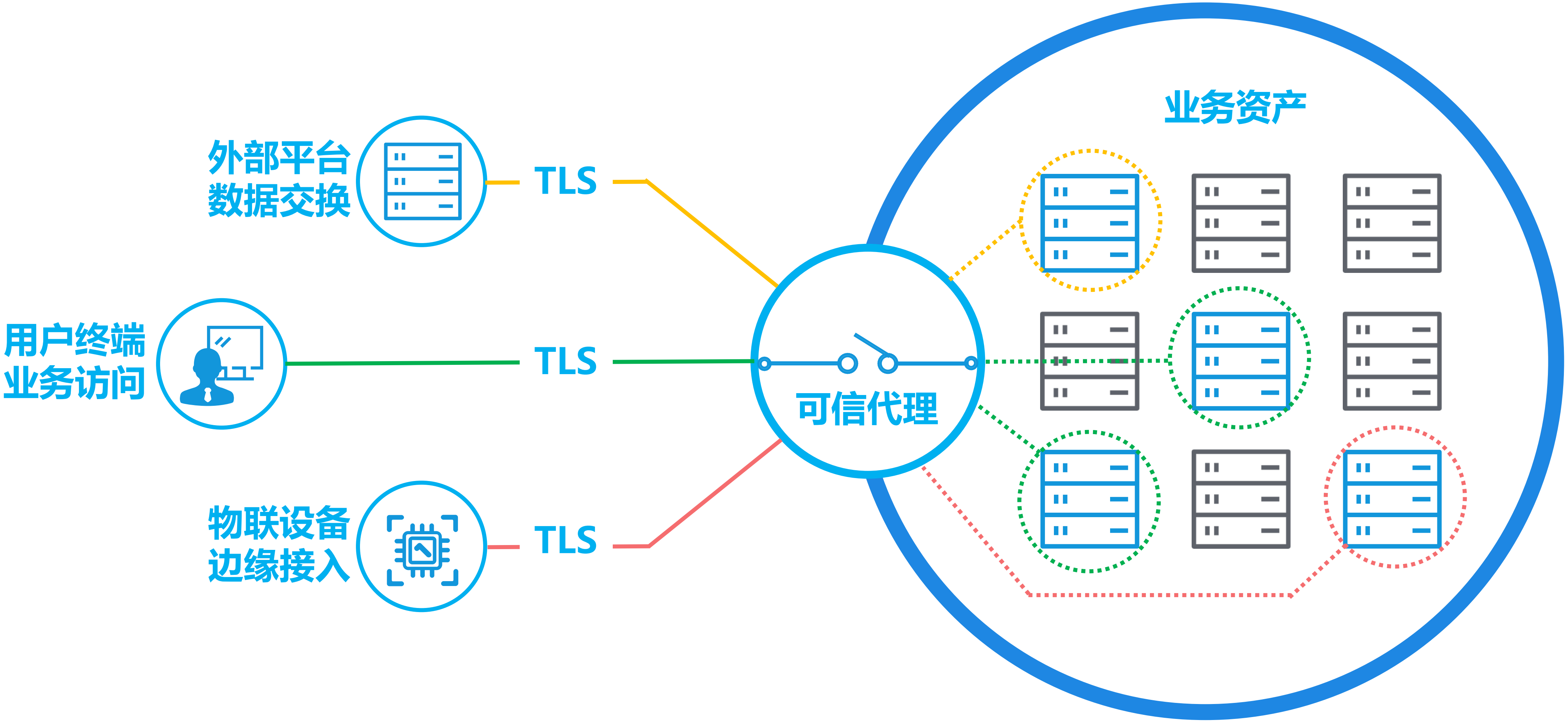




业务访问主体

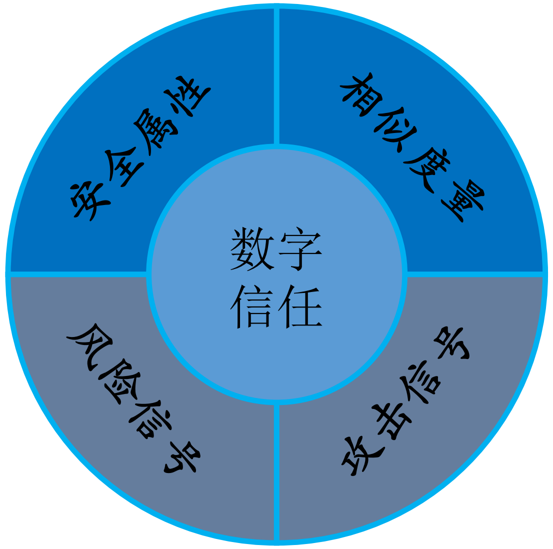
完整不可分割

业务安全访问



全场景业务隐藏　全流量加密代理　全业务强制授权

持续信任评估

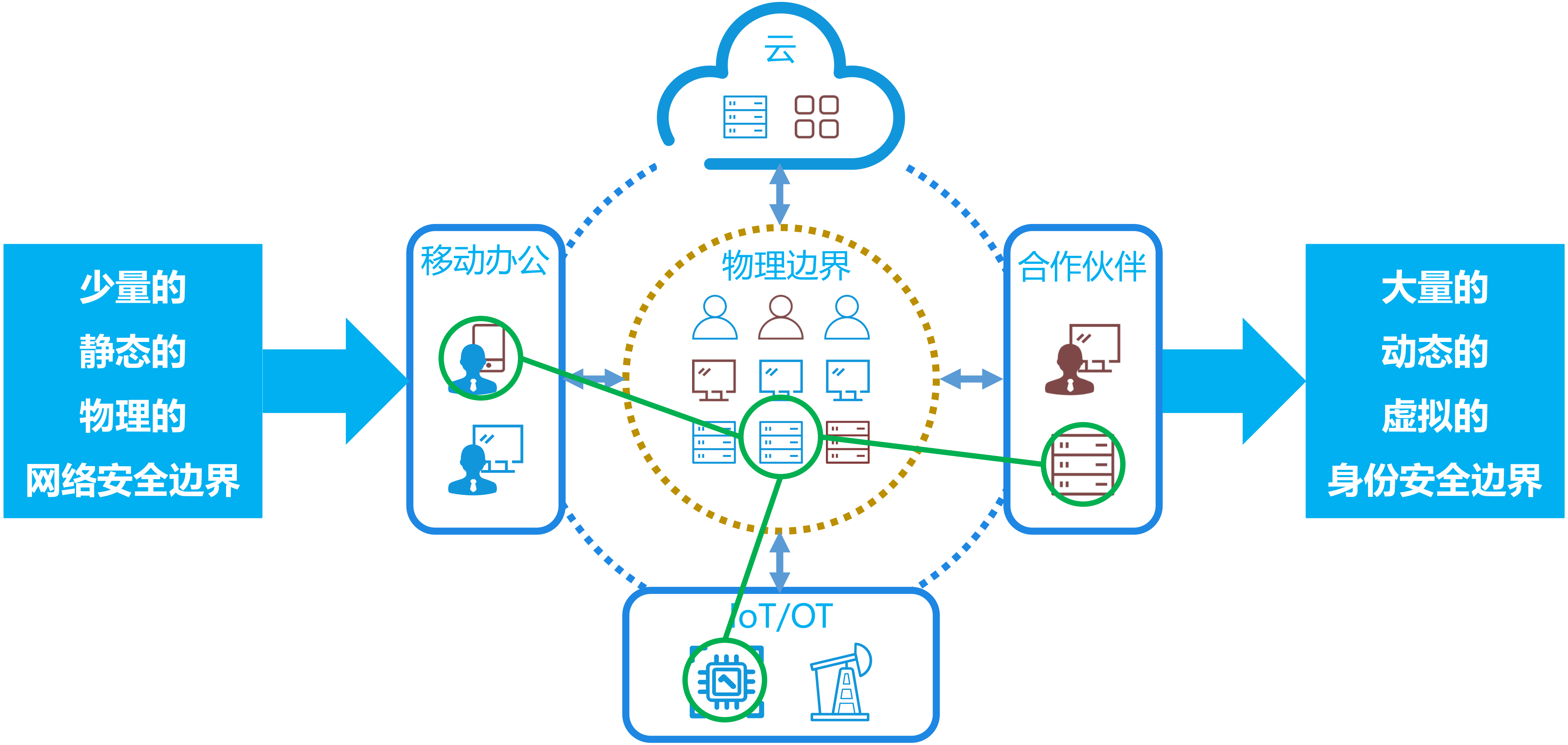


身份的数字信任

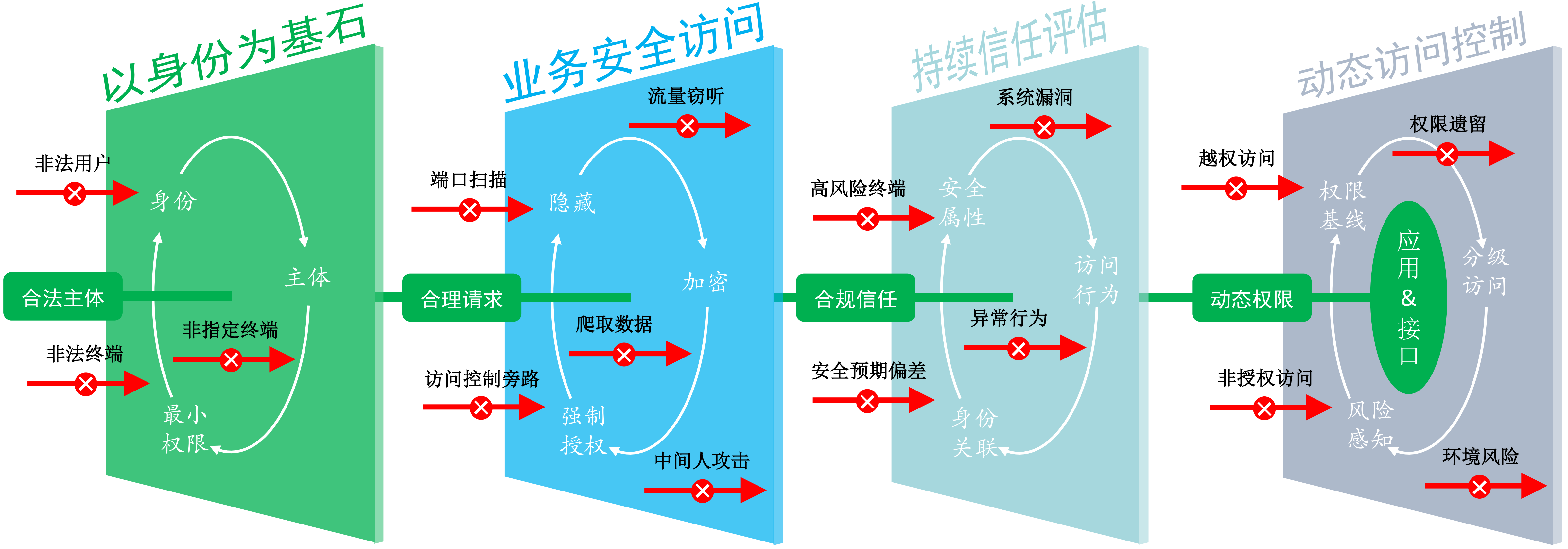
动态访问控制

环境
信任等级
主体
环境
安全等级
客体
基于属性的访问控制基线
基于风险感知的动态权限
提升信任|缓解风险|拒绝访问
基于信任等级的分级访问
当主体信任等级大于客体安全等级时，访问权限才真正授予
人
设备
应用
环境
信任评估因子
风险感知
威胁
价值
环境
安全等级

构筑以身份为基石的动态虚拟边界

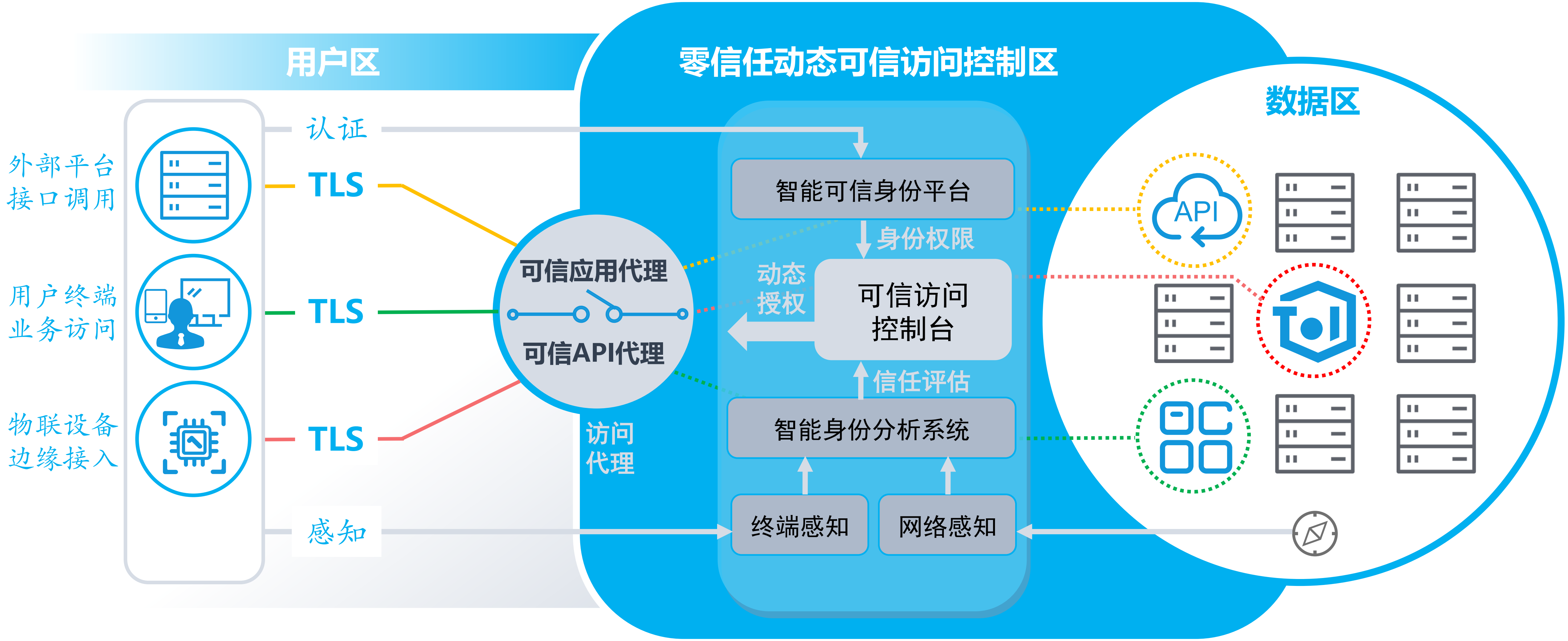


安全价值：收缩攻击面、缓解高风险



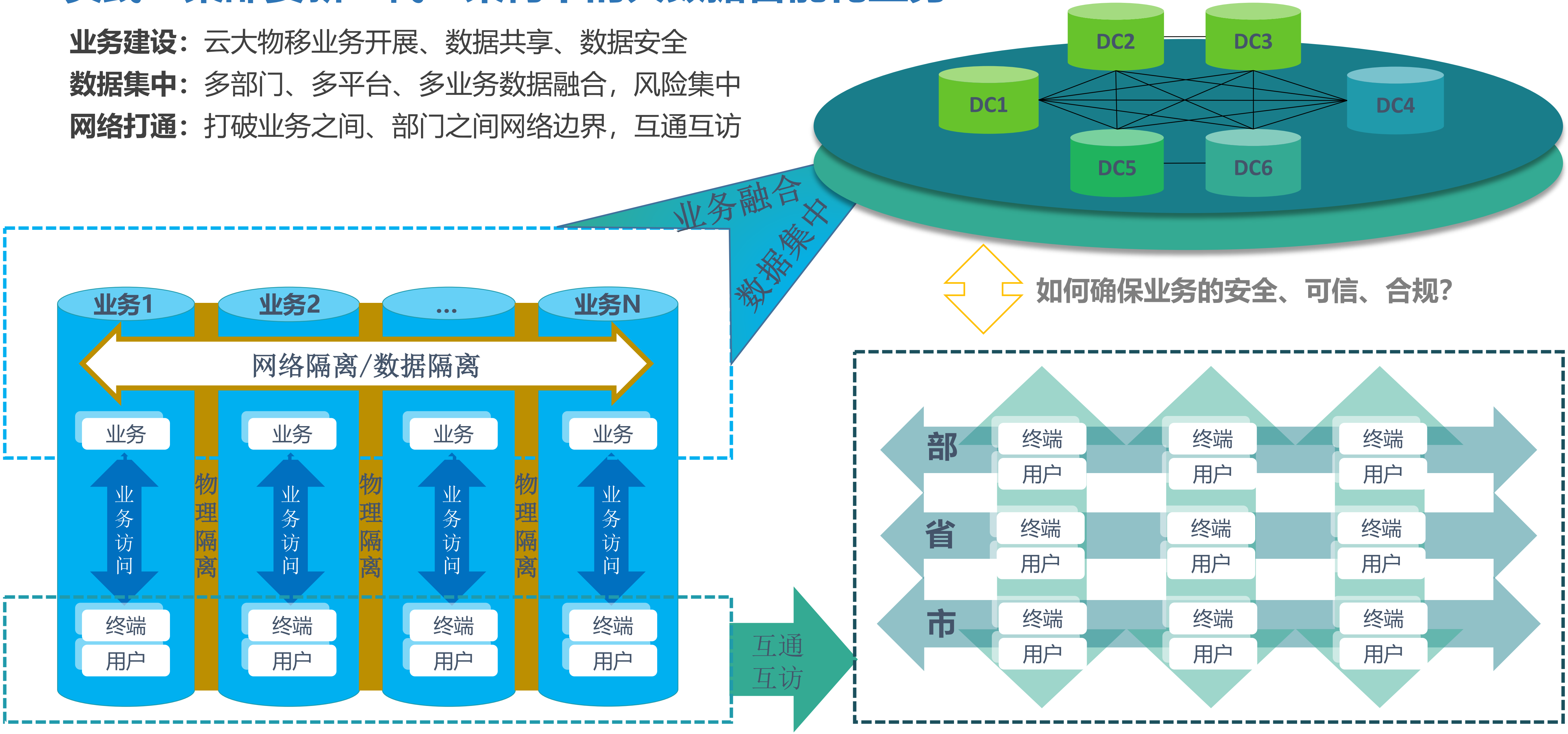
全面身份化　风险度量化　授权动态化　管理自动化

奇安信零信任身份安全架构

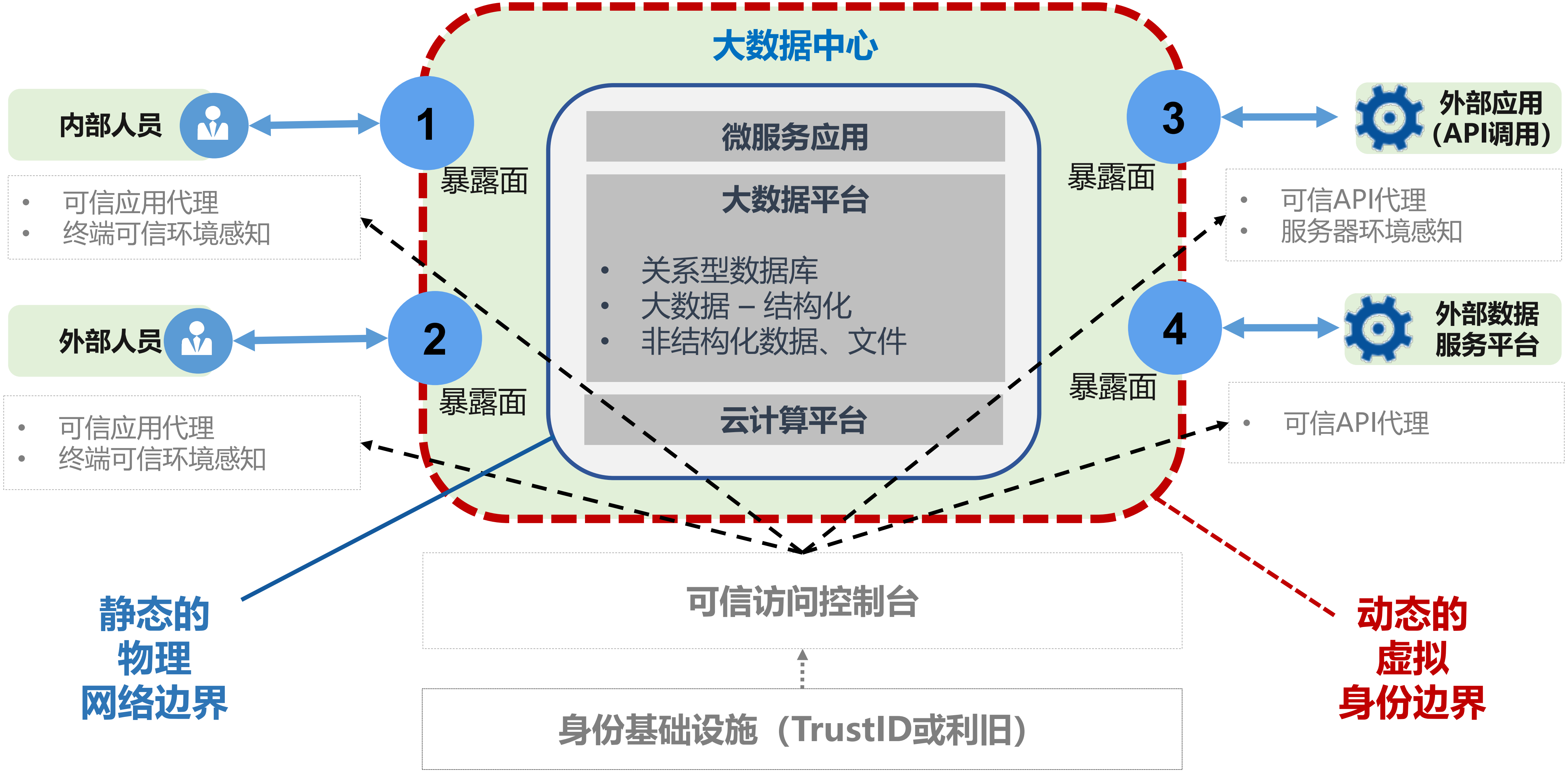


实践：某部委新一代IT架构下的大数据智能化业务

业务建设：云大物移业务开展、数据共享、数据安全
数据集中：多部门、多平台、多业务数据融合，风险集中
网络打通：打破业务之间、部门之间网络边界，互通互访

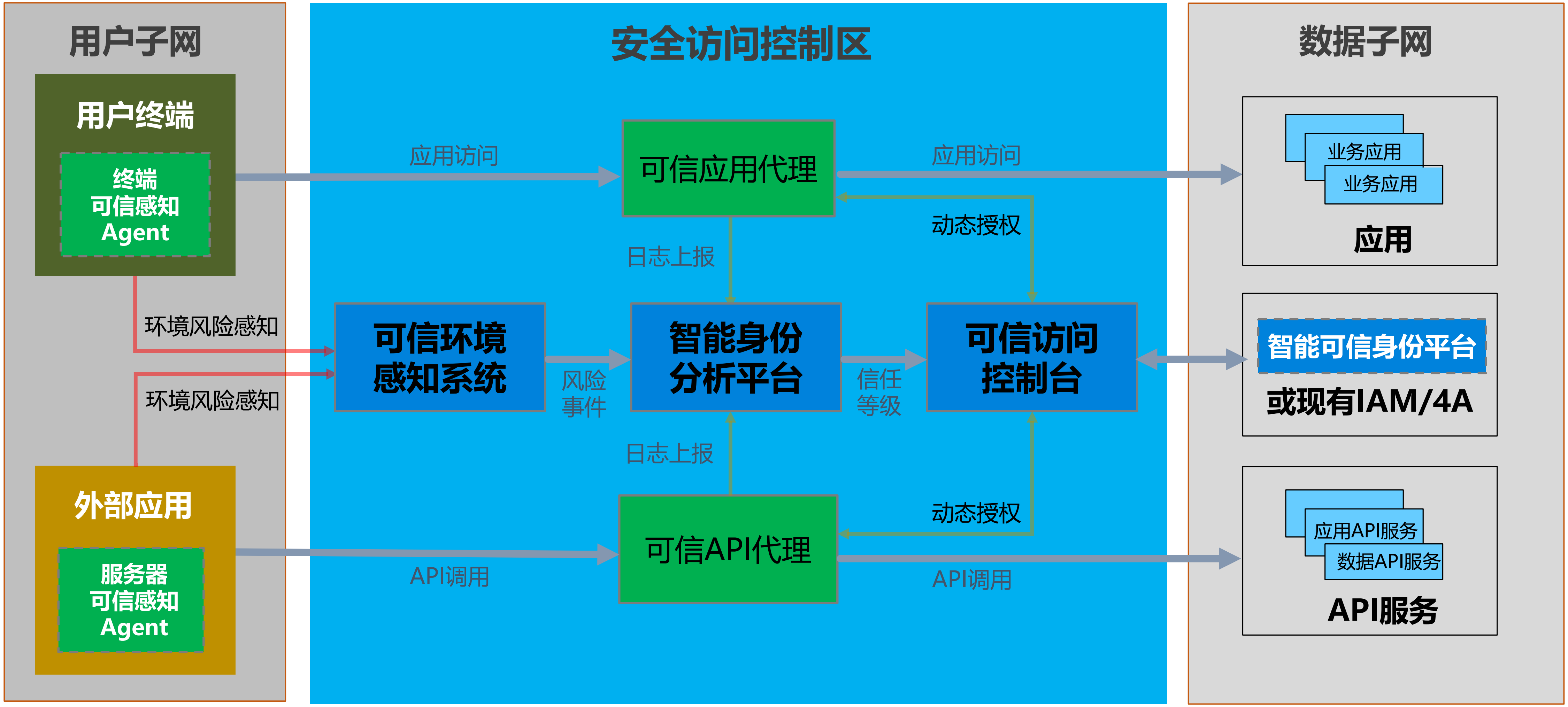


实践：梳理核心资产的访问路径，构建虚拟身份边界

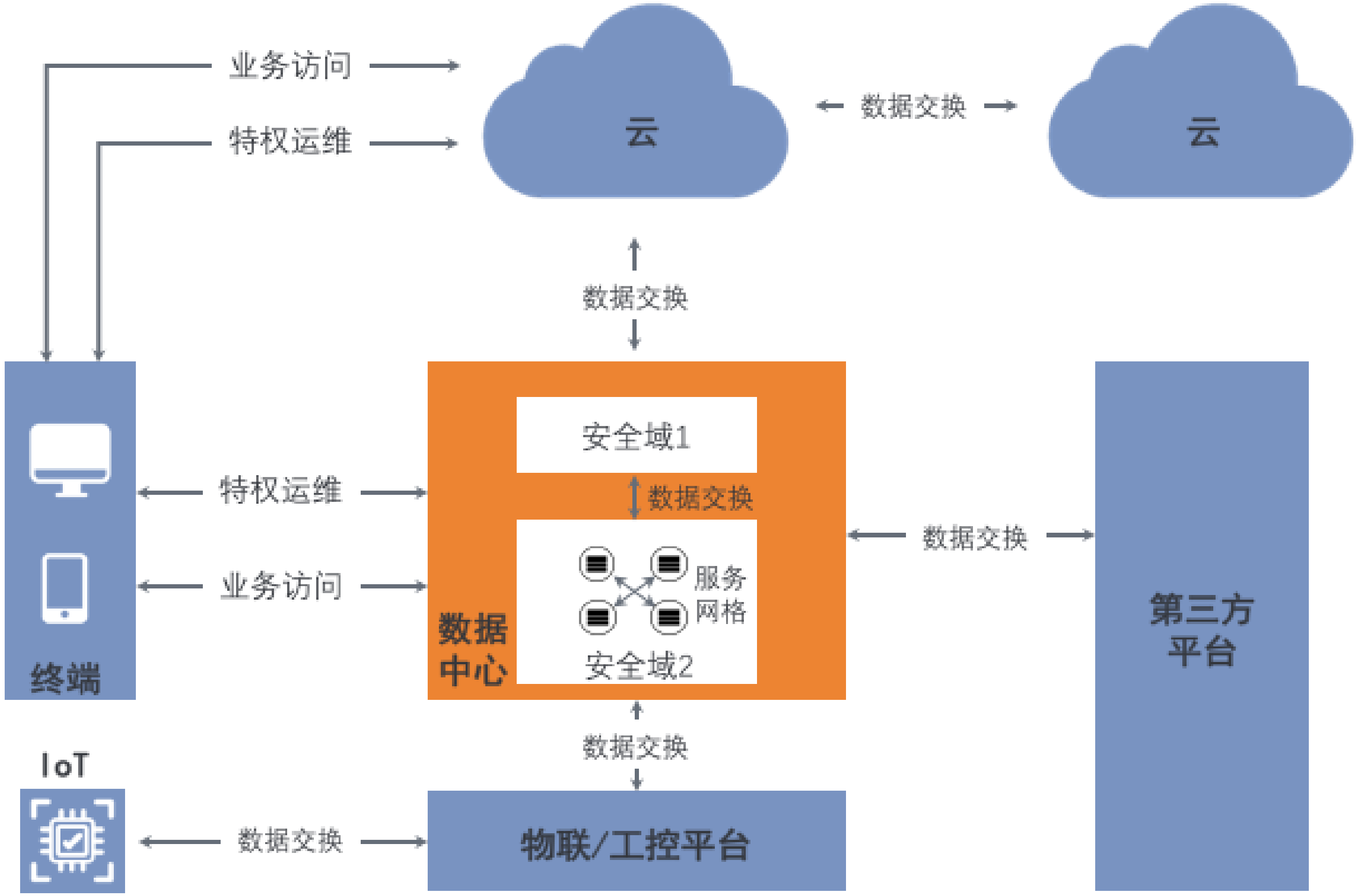


实践：基于零信任架构的动态可信安全访问平台

基于零信任架构设计，大数据子网不再暴露物理网络边界，建设跨网安全访问平台隐藏业务应用和数据。

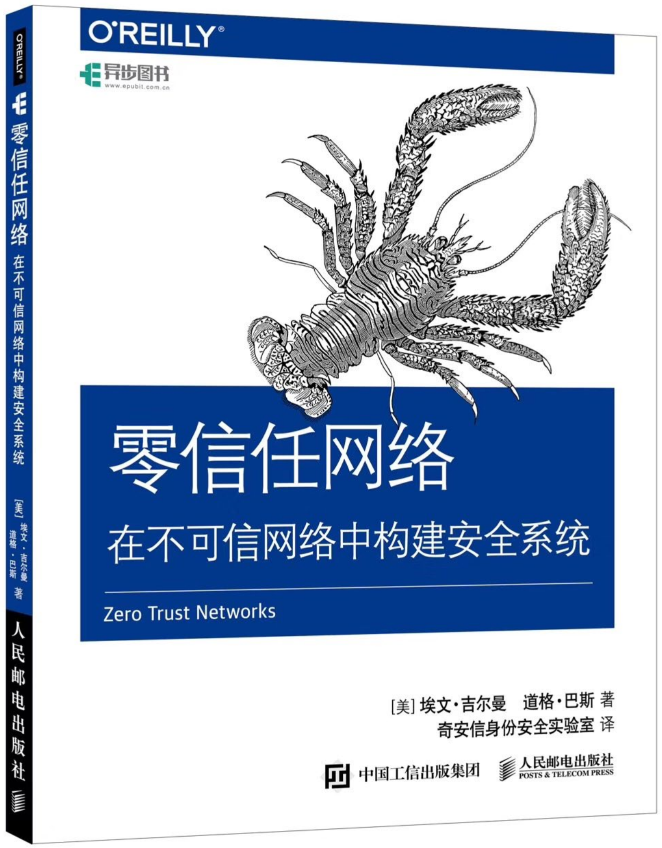


工程化视角的展望



1. 信任评估模型
2. 更多的传感器和数据
3. 安全效果可视化
4. 弱感知技术
5. 自身安全性
6. 高可用/高性能

欢迎交流



零信任安全社区

安全内参
网络安全首席知识官

深度解读零信任身份安全专栏

奇安信身份安全实验室出品，专注"零信任身份安全架构"研究。

XDef 2019

对话 · 交流 · 合作　　前沿 · 实用 · 人才

Thanks

谢谢关注！